WEB MANAGERS HELP · FREE CHECKLIST

The Accidental Web Manager's First 30 Days

You got handed the website. This is what to do in the first month, in order. Drawn from *Strategic Web Management: First Steps for the Accidental Web Manager* by Bryan C. Mills, and from twenty years of arriving after the "aw, man."

FREE · v1.0 · 2026

Thirty days, four weeks, one question: if something important broke tonight, could the organization get back in? Nothing on this list is visible to the public. That is the point. New web managers tend to skip this month for cosmetic wins, and it is precisely the month that decides whether the site survives its next bad day.

1 BOOK THE HOUR

One recurring **two-hour appointment** a week, on the calendar, defended. Intentions do not survive contact with a calendar; appointments do.

2 FIND

Inboxes, statements, DNS, the last person who did this. **Log everything, fix nothing yet.** Judgment comes after the list exists.

3 SECURE

Move every login into a vault, re-anchor accounts to an address the organization controls, and **turn on 2FA** where it matters most.

4 PROVE IT

Each week ends with a **definition of done you can test**, not a feeling. Day 30 closes with three disaster drills on paper.

HOW TO USE THIS CHECKLIST

- Work the weeks in order. Each one is the ground the next stands on.
- Every task has a "done looks like." If you cannot point to it, the task is not done.
- Hours are honest estimates for one person with no help. The two-hour appointment plus a couple of pushed evenings covers it.
- Record what you find on page 4 as you go, not at the end.

Total: roughly 20 hours across the month.

THE THREE DISASTERS THIS MONTH PREVENTS

Lost password	The only person who could log in is gone, or it was you, and the recovery email goes to a phone that left with them.
Expired card	The domain or hosting renews on a card nobody has, the notices go to an inbox nobody reads, and the site simply stops.
Dead server	The host has a bad day and the only backup lives on the same server, or there is no backup, or nobody has ever tested one.

Most inherited websites end one of these three ways.

YOUR 30 DAYS

STATUS: ◯ Not started ◯ In progress ◯ Day 30 passed

WEB MANAGER _____ **DAY 1** _____

ORGANIZATION _____ **DAY 30** _____

The engine (do this first): recurring two-hour weekly appointment booked ☐ role-based email address created ☐

WEEK 1 · DAYS 1–7

Confirm the Job

~2 HRS

Scope confirmed early is scope that cannot ambush you later.

TASK	DONE LOOKS LIKE	EST. HRS	DONE
Write the one-sentence job description and send it to your boss or board: "I am responsible for keeping our digital presence (website, domains, email, and connected accounts) secure, current, and serving [organization]'s mission, with a budget and vendors to match."	A reply, in writing, that agrees or corrects it. File it. It is your first piece of role documentation.	0.5	☐
Score what you know against what you own. For each of website, domain, hosting, email, social, and analytics, answer two questions: can I log in today, and is it my responsibility?	A dated six-row list with a yes or no in each column. The "no, and yes" rows are your month.	0.5	☐
Create a role-based email address the organization controls (webmaster@ or web@) and forward it to yourself. Every account you touch this month gets re-anchored to it.	The address exists, delivers to you, and its password is not only in your head.	0.5	☐
Find your predecessor (or their auto-reply, or their sticky note) and ask three questions: where are the logins, who do we pay, and what breaks.	Their answers written down, dated, and filed, even if the answers are "I don't know."	0.5	☐

Definition of done (test it, don't feel it):

☐ Someone with authority has confirmed in writing what you are responsible for, ☐ the weekly appointment is on the calendar, ☐ the role address works.

WEEK 2 · DAYS 8–14

Find Everything

~6–8 HRS

Go forage. Log every service you find without judging or fixing anything yet.

TASK	DONE LOOKS LIKE	EST. HRS	DONE
Search the main inboxes for "renewal," "invoice," and "verify your account." Log every distinct service as its own row.	Twenty minutes usually surfaces most of your accounts and at least one surprise.	1	☐
Pull twelve months of card and bank statements and log every web-related charge: hosting, domains, plugins, email tools, "the $12.99 one."	Every recurring charge matched to a service on the list, or flagged as unknown.	1	☐
Look up your domain at lookup.icann.org. Note the registrar, the registrant, and the expiration date.	You can name the company the domain is registered with and the date it expires.	0.25	☐
Identify what the site runs on (BuiltWith or Wappalyzer, free) and who hosts it. The host is the one to call when the site is down but email still arrives.	Platform and host written on the inventory. You know which landlord to call.	0.25	☐
Snapshot the DNS records wherever DNS is managed (usually the registrar or host). Screenshot or export the whole zone and file it, dated.	A dated file you could hand to a technician if every record vanished tomorrow.	0.5	☐
Build the inventory. One row per service: name, what it does, who owns the login, which email it is tied to, payment method, renewal date, notes.	One spreadsheet, one row per service, no blanks in the "who owns the login" column.	2–3	☐
Flag the risky rows. Mark every account tied to a personal email, an ex-employee, a vendor's account, or a recovery method nobody controls.	A flag column. The flagged rows are next week's work, in order of how much would break.	0.5	☐

Definition of done (test it, don't feel it):

☐ A single dated list of every service exists, ☐ every recurring charge is matched to a row, ☐ every risky row is flagged.

WEEK 3 · DAYS 15–21

Take the Keys

~6 HRS

The organization holds its own logins, and two people besides you could get in tomorrow.

TASK	DONE LOOKS LIKE	EST. HRS	DONE
Stand up a password vault (Bitwarden's free tier is enough) and move every credential from the inventory into it. Then delete the spreadsheet of passwords, ceremonially.	Every login lives in the vault; the old spreadsheet, sticky note, or shared doc is gone.	2–3	☐
Re-anchor the flagged accounts to the role address: registrar first, then host, then everything else. For any you cannot reach, start the platform's recovery process now, politely and promptly.	Flagged rows cleared or marked "recovery in progress" with a date.	2	☐
Count your website administrator accounts. Demote everyone who does not strictly need admin, delete accounts of people who have left (after noting anything they own), and turn on 2FA for the rest. Repeat at the hosting account.	As few admins as possible, all of them current people, all with 2FA.	0.5	☐
Turn on 2FA at the registrar and DNS provider, with the second factor held by the organization, not a phone that leaves when someone does.	2FA on for the three accounts that can take the whole site down; backup codes in the vault.	0.5	☐
Write the "hit by a bus" one-pager: where the inventory is, where the vault is, who holds emergency access, who to call. Date it. Store it. Tell two people.	One page, two people who know where it is, neither of them you.	1	☐

Definition of done (test it, don't feel it):

☐ Two people other than you could get into everything tomorrow, ☐ no password lives only in someone's head or a spreadsheet, ☐ no admin belongs to someone who has left.

WEEK 4 · DAYS 22–30

Survive the Three Disasters

~4–5 HRS

Renewal defenses, a tested backup, and an alarm that reaches you before a customer does.

TASK	DONE LOOKS LIKE	EST. HRS	DONE
Domain renewal defenses. Auto-renew on; the card on file verified current (add a backup card if the registrar allows); registrar transfer lock on; expiration at least 90 days out, ideally two to five years.	Independent calendar reminders at 60, 30, and 7 days before expiration, on a calendar the organization owns.	1	☐
Backups: confirm, then test. Find out whether a backup exists, where it lives, and that at least one copy is not on the same server as the site. Then restore one file or page from it.	A dated note: backup location, how often it runs, restore test date, result, your signature.	2	☐
Uptime monitor. Create a free UptimeRobot account and add a monitor for the homepage, with alerts to the role address and, if you like, your phone.	From this day forward you learn the site is down from a notification, not a customer.	0.5	☐
Ten-minute email check. Paste your domain into MXToolbox's SPF and DMARC checkers. Green on both means your mail is authenticated; red on either means some share of everything you send is being silently filtered.	A note that says green or red. Red is your first project after day 30, and probably the highest-return afternoon you will spend.	0.25	☐
Report upward, one page. What you found (in before-language), what is now true, and the one thing you need next: time, budget, or a decision.	Leadership has read one page they did not ask for, and it ended with a specific ask.	1	☐

Definition of done (test it, don't feel it):

☐ The organization would survive a lost password, ☐ an expired card, ☐ and a dead server, this week, without you being reachable.

DAY 30 · RUN THE THREE DRILLS ON PAPER

☐	**I lost my password tonight.**	Who else can get into the registrar, the host, and the website by tomorrow morning, without calling me? **Name them:** _____
☐	**The card on file expired.**	Which reminder would fire first, on whose calendar, and how many days before the domain went dark? **Answer:** _____
☐	**The server died this afternoon.**	Where is the most recent backup that is not on that server, and when was a restore last tested? **Date:** _____

What You Found

Recordeverysurpriseasyougo: the mystery charge, the account in an ex-employee's name, the backup that does not exist. This is your first fix list.

PRIORITY	WHAT YOU FOUND	WHAT NEEDS TO HAPPEN	TARGET DATE	DONE
◆ Now ▲ Month ● Later				☐
◆ Now ▲ Month ● Later				☐
◆ Now ▲ Month ● Later				☐
◆ Now ▲ Month ● Later				☐
◆ Now ▲ Month ● Later				☐
◆ Now ▲ Month ● Later				☐
◆ Now ▲ Month ● Later				☐

◆ Now: could take the site down ▲ Month: costs money or access if ignored ● Later: hygiene, schedule it

DAY 31 AND AFTER
You are not alone in this. What comes next.

LISTEN

The Web Managers Podcast. Episode 1 is the audio version of this checklist: the same month, with the stories behind each task. Search for it wherever you listen, or find the link at **webmanagers.com**.

READ

Strategic Web Management: First Steps for the Accidental Web Manager by Bryan C. Mills. This checklist is its first 30 days; the book carries the next 60 and the year after, with a worksheet for every chapter.

FOLLOW

@webmanagershelp on Instagram: one recognizable moment and one fix at a time, three times a week. Tag the person who got handed the website.
#AccidentalWebManager